(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 June 2002 (27.06.2002)

PCT

(10) International Publication Number
WO 02/51096 A1

(51) International Patent Classification[7]: H04L 29/06, H04N 7/167

(21) International Application Number: PCT/IB01/02406

(22) International Filing Date: 10 December 2001 (10.12.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data: 00204639.9 18 December 2000 (18.12.2000) EP

(71) Applicant: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventor: VAN RIJNSOEVER, Bartholomeus, J.; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agent: HOEKSTRA, Jelle; International Octrooibureau B.V., Prof Holstlaan 6, NL-5656 AA Eindhoven (NL).

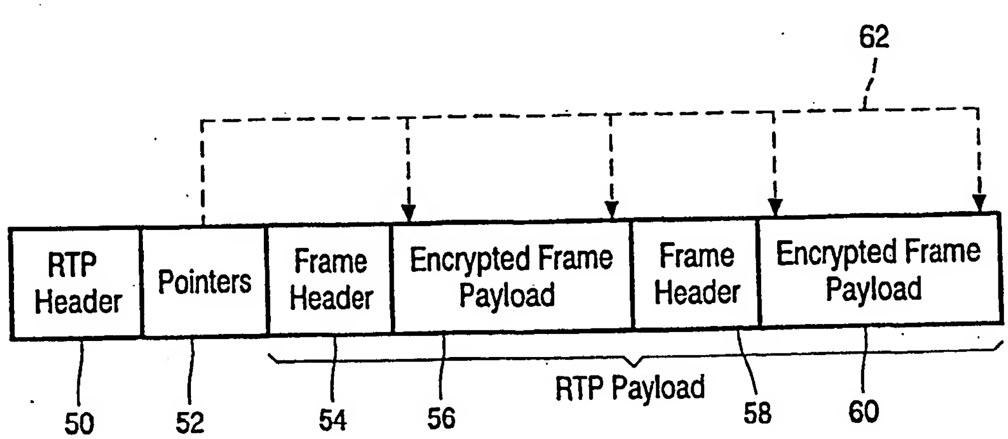
(81) Designated State (national): JP.

(84) Designated States (regional): European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: POINTERS TO ENCRYPTED DATA IN RTP HEADER



(57) Abstract: Frame-formatted user data is real-time transmitted whilst thereon effecting before transmission a frame-based encryption procedure. In particular, before subjecting to the encryption procedure, localizing data is joined to the data frame and placed into predetermined governance locations that are excluded from the subsequent encrypting.

WO 02/51096 A1

Pointers to encrypted data in RTP header

A method and system for real-time transmitting frame-formatted user data through joining thereto frame localizing data placed in predetermined governance locations, whilst before transmission effecting an encryption procedure that excludes said localizing data, and a system, a transmitter apparatus, a receiver apparatus, and a signal produced by such transmitter apparatus for use with such method.

BACKGROUND OF THE INVENTION

The invention relates to a system as recited in the preamble of Claim 1. Data, and in particular, but not restricted to, multi-media data are at present being encrypted for implementing inter alia various conditional access schemes to allow creators and distributors of the original matter to collect an appropriate amount of retributions from users of such information. At the receiver side, the user data must be recuperated in order to allow for orderly representing, viewing, listening, executing, and other user-associated operations. The actual transmission via some transmission medium, such as a network, will take place on a packetized level, where the packets are standardized for the network or networks in question.

A first approach is to effect the encryption on the basis of a Real Time Protocol transmission packet, which is a relatively simple procedure and is alright for protecting the transmission proper. Alternatively, a higher protection level can be attained that will also remain in force at the receiver side: this can be done by having the encryption implemented on the basis of the frame structure of the source data or user data. It is also feasible to implement a combination of the two above approaches. Now, the encryption should advantageously be executed in a standard component that should not need to effect complicated preprocessing to find the start of a frame. Therefore, all of the above procedures will need an easy mechanism to straightforwardly find the beginning of the frames.

SUMMARY TO THE INVENTION

In consequence, amongst other things, it is an object of the present invention to add specific localizing information to allow the encoder mechanism and possibly, also the decoder mechanism to quickly and easily find the start of the various frames.

Now therefore, according to one of its aspects the invention is characterized according to the characterizing part of Claim 1.

Further to the above, the present inventor has recognized that a slight modification to the above may allow to have only a part of the user data being effectively encrypted, whilst still enabling the immediate localizing of the various such encrypted parts, as has been recited in Claim 2. The invention also relates to a system being arranged for implementing the method as claimed in Claim 1, to a transmitter apparatus and to a receiver apparatus for use in such system, and to a signal produced by such transmitter apparatus. Further advantageous aspects of the invention are recited in dependent Claims.

BRIEF DESCRIPTION OF THE DRAWING

These and further aspects and advantages of the invention will be discussed more in detail hereinafter with reference to the disclosure of preferred embodiments, and in particular with reference to the appended Figures that show:

Figure 1, a system arranged for implementing the inventive method;

Figure 2, a data format implementation for use in the present invention;

Figure 3, an amended format with respect to Figure 2 that has partial encrypting.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

The quality of content information, such as audio or video on the Internet is improving due to steady advances in coding technology and in transmission bandwidth. Content providers intend to sell such high value content, and therefore, a need is arising for effecting conditional access or digital rights management, as it is called. Such conditional access system will encrypt a content item and will subsequently manage the associated decryption keys in such manner that only authorized end users will be able to decrypt and thereby reconstitute the original content in full.

Now, multi-media data is generally structured in frames, wherein the size of a frame is related to the category of information. Furthermore, the size of a transmitted frame may

relate to the degree of compaction and other processing it has been subjected to before encryption. In fact, the frames may be larger as well as smaller than the packets used for actual transmission. Therefore, a single transmission packet may contain one or more frames, or fractional parts of a frame. ***Streaming*** is a technology wherein a client will play or otherwise use the content as soon as it will arrive, so there will be no downloading of all, or a substantial part of, an entire content before playing. Streaming will not allow for retransmission of packets. The content user will have to cope with the occurrence of lost data.

Now for optimum protection, content is best encrypted at the frame level, even with non-uniform frame size. Such encryption at the frame level will allow for persistent or end-to-end encryption that applies to both transmitted as well as to stored content. Preferably, the system component that implements the actual encryption is a generic component, and should therefore be independent of specific streaming servers and independent of specific frame formats. One way to achieve this is to define the encryption component as a Realtime-Transmission-Protocol- or RTP-translator. At present, virtually all streaming servers are using the RTP streaming protocol. Therefore, the encryption component could receive the RTP packets, encrypt the payload, and subsequently forward the encrypted RTP packets. Alternatively, the encryption may be integrated with the streaming server.

Alternatively, the encryption may be executed on the level of the RTP-packet. This will protect the transmission proper, whilst surrendering part of the protection at the receiver side after receiving. Also, a combination of these two encryption approaches is feasible, such as by assigning the appropriate encryption level on the basis of a contingency strategy viz à viz available hardware facilities.

A problem is posed in that the headers of the frames must remain unencrypted, such as when the encryption is effected at the frame level. This requires that the generic encryption component should analyze the payloads of the RTP packets to identify the positions of the frame headers. Such would however lower the performance of the encryption component, and will also make the encryption component dependent on actual frame formats.

The present invention provides a solution to the problem in question by extending the headers of RTP packets to include pointers to those parts of the RTP packet payload that actually need to be encrypted. The pointers are set by the streaming server. The server may do this as part of the so-called hint process, that is an off-line analysis of multi-media data, so that the data may be streamed more efficiently at a later instant in time. The result of the hint process is stored in parallel to the content in a so-called hint track.

Figure 1 illustrates a system arranged for implementing the inventive method. Input 23 receives the user data frames, that are transiently stored into storage 22, which accommodates storage of a plurality of such frames. Processing block 24 thereupon joins to these data frames frame header localizing informations in the context of an RTP packet that may comprise a plurality of such user frames, but not necessarily an integer number thereof. The result of this processing is transiently stored in block 26 that accommodates multiple RTP payloads. For brevity, the specific *hint* track mentioned supra has not been shown separately. In fact, the hint track facility will be recognized by persons skilled in the art as a standard facility. In practice, such hint track will be implemented at the input side of block 23 to allow indicating the various frame locations. Before transmission, the user data are encrypted in encryption module 28 and transmitted over communication facility 30, such as Internet. The whole procedure at the transmitter side of the system shown may be synchronized by overall synchronization facility 20 as indicated by dashed lines leading therefrom.

At the receiving side, decryption is effected through decryption facility 34, and the result thereof is transiently stored in block 36. Reconstitution of the user frames is effected in processing facility 38, followed by transiently storing in block 40. User application is then symbolized by block 42. Storage blocks 36, 40 do not accommodate downloading of a complete program or a substantial part thereof, but rather will provide for some synchronizing to cater for transfer speed variations of communication facility 30. Again, at the receiver side, overall synchronization is effected through synchronizer block 32.

Figure 2 illustrates an exemplary data format implementation for use in the present invention. For brevity, only a single implementation has been shown. Various data blocks 50-60 of the RTP configuration have been shown in the Figure. Of these, blocks 54-60 constitute the RTP payload, wherein blocks 56, 60 each contain an encrypted frame payload, and blocks 54, 58 contain the associated frame headers. Note that the lengths of blocks 56, 60 need not be uniform. Block 50 contains an RTP header, and is followed by block 52 that contains pointers. As shown in the figure, the pointers 62 indicate both the beginning and the end of each encrypted frame payload. Now, the header 50 is found in the hint track; pointers 52 are extensions of the RTP header 50. This hint track is used by the streaming server for packaging the RTP packets.

Figure 3 illustrates an amended format with respect to Figure 2 that has partial encryption of the user data. For brevity, only the aspects that differentiate from Figure 2 have been indicated specifically. Within the frame payload, the discrimination between encrypted (E) and unencrypted user data has been indicated by a slanted line. The localizing information

indicated by 62 in this case will now specifically indicate (63, 65) the ends of the respective encrypted parts, assuming that the encryption starts from the beginning of the frame's user data. Of course, other partial encryptions may be used. The encryption itself may be done on the level of a frame or partial frame, on the level of a packet, or be based on a combination thereof.

CLAIMS:

1. A method for real-time transmitting or retransmitting frame-formatted user data whilst thereon effecting before such (re-)transmitting an encryption procedure,

said method being characterized by the step of, associated to subjecting said user data to said encryption procedure, joining to said user data appropriate frame localizing data and placing such frame localizing data into predetermined governance locations which, just as well as header informations, are excluded from subsequent said encryption procedure.

2. A method as claimed in Claim 1, whilst subjecting only a part of said user data to said encryption procedure whilst providing for encryption localizing data in said governance locations to discriminate between encrypted and non-encrypted parts of said user data.

3. A method as claimed in Claim 1 or 2, wherein such governance locations are header extension information locations.

4. A method as claimed in Claim 1 or 2, wherein said user data after encryption are transmitted in RTP-packets, and wherein said user data are encrypted on a level of said RTP packet.

5. A method as claimed in Claim 1 or 2, wherein said user data are encrypted on a frame level.

6. A method as claimed in Claims 4 or 5 wherein said transmission allows for imparting partial frames to a packet, as well as allowing to impart a plurality of frames to a single packet.

7. A method as claimed in Claim 3, wherein such header extension information location has a plurality of frame localizing data.

8. A method as claimed in Claim 1 or 2, wherein such governance locations are placed within a separate hint track.

9. A system arranged for implementing a method as claimed in Claim 1 and having transmission means for real-time transmitting or retransmitting frame-formatted user data and encryption means for effecting before such (re-)transmitting an based encryption procedure on said user data,

said system being characterized by comprising next to said encryption means joining means for joining to said user data frame localizing data and placing such frame localizing data into predetermined governance locations which, just as well as header informations, are excluded from subsequent said encryption.

10. A system as claimed in Claim 9, and being arranged for interfacing to Internet as a transmission medium.

11. A transmitter apparatus being arranged for use as a station in a system as claimed in Claim 9.

12. A signal produced by a station as claimed in Claim 11.

13. A receiver apparatus being arranged for use as a station in a system as claimed in Claim 9 and having decryption means for upon reception decrypting user data that had been subject to said encryption procedure for outputting user data so decrypted as based on frames containing said user data.

14. A receiver apparatus as claimed in Claim 13, wherein said decryption means are operational on a frame level.

15. A receiver apparatus as claimed in Claim 13, wherein said decryption means are operational on a packet level.

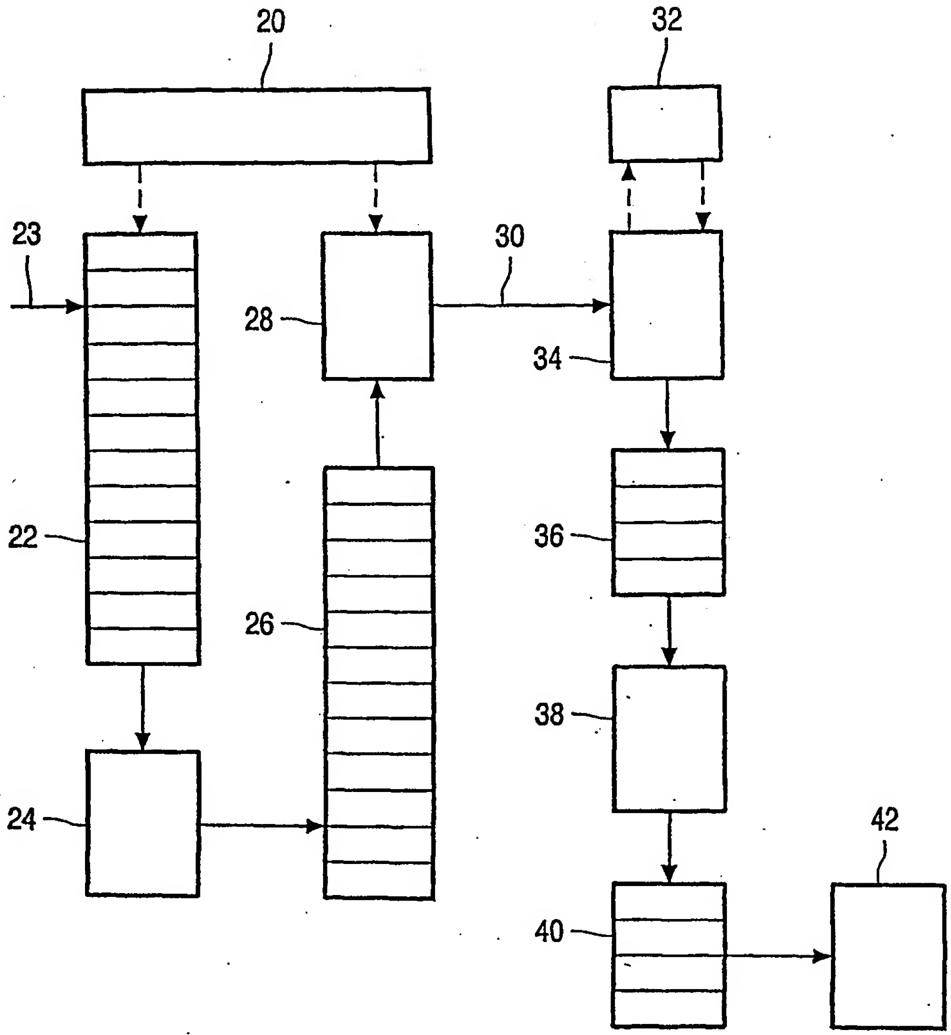


FIG. 1

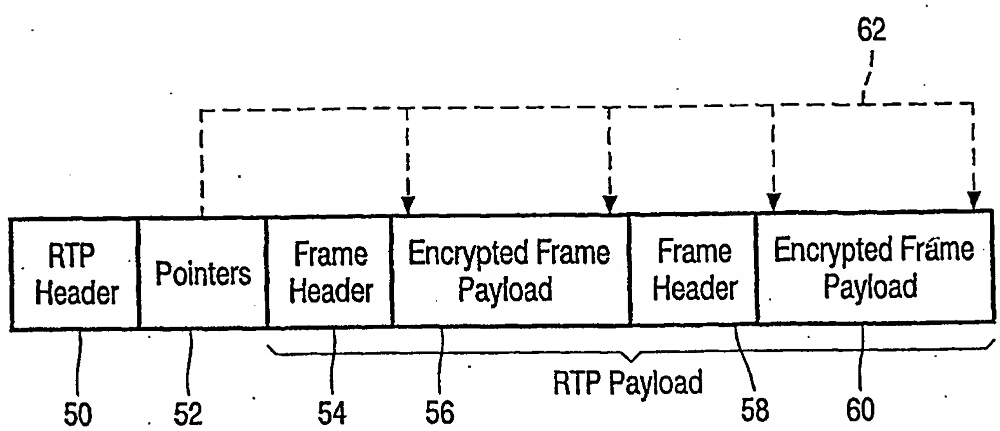

62
RTP Header
Pointers
Frame Header
Encrypted Frame Payload
Frame Header
Encrypted Frame Payload
RTP Payload
50
52
54
56
58
60

FIG. 2

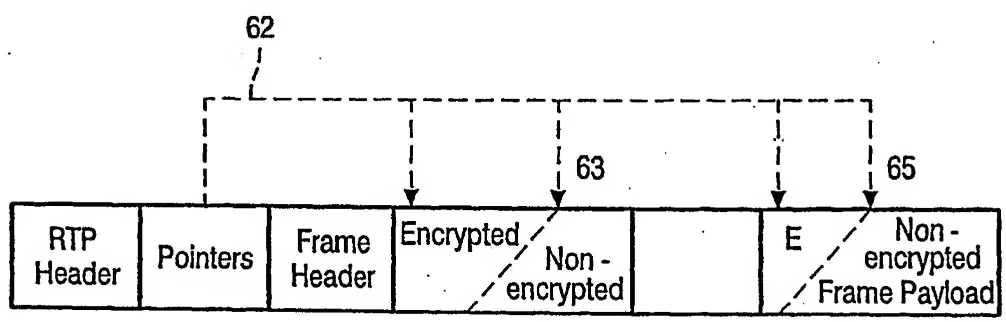

62
63
65
RTP Header
Pointers
Frame Header
Encrypted
Non - encrypted
E
Non - encrypted Frame Payload

FIG. 3

PCT/IB 01/02406

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04N7/167

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 99 37056 A (APPLE COMPUTER) 22 July 1999 (1999-07-22) page 20, line 6 - line 7 page 38, line 9-12	1,9
A	US 5 953 418 A (TAPU MARIAN ET AL) 14 September 1999 (1999-09-14) figure 14	1,9

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
31 May 2002	11/06/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Tito Martins, J

Patent document cited in search report		Publication date	Patent family member(s)			Publication date
WO 9937056	A	22-07-1999	AU	2232799	A	02-08-1999
			AU	2232899	A	02-08-1999
			AU	2322499	A	02-08-1999
			CA	2316852	A1	22-07-1999
			CA	2318963	A1	22-07-1999
			CA	2325828	A1	22-07-1999
			CN	1308437	A	15-08-2001
			CN	1290444	T	04-04-2001
			CN	1290445	T	04-04-2001
			EP	1051008	A2	08-11-2000
			EP	1048156	A2	02-11-2000
			EP	1062782	A2	27-12-2000
			JP	2002510165	T	02-04-2002
			WO	9937056	A2	22-07-1999
			WO	9937057	A2	22-07-1999
			WO	9937072	A2	22-07-1999
			US	6134243	A	17-10-2000
US 5953418	A	14-09-1999	US	5869279	A	09-02-1999
			WO	9700328	A1	03-01-1997
			US	5770404	A	23-06-1998
			AU	6477596	A	15-01-1997
			CA	2224238	A1	03-01-1997
			EP	0832525	A2	01-04-1998
			WO	9700564	A2	03-01-1997
			US	5802311	A	01-09-1998
			US	5948119	A	07-09-1999

US005805700A

United States Patent [19]

Nardone et al.

[11] Patent Number: 5,805,700

[45] Date of Patent: Sep. 8, 1998

[54] **POLICY BASED SELECTIVE ENCRYPTION OF COMPRESSED VIDEO DATA**

[75] Inventors: **Joseph M. Nardone**, Portland, Oreg.; **Keith L. Shippy**, Tempe, Ariz.; **David W. Aucsmith**, Portland, Oreg.

[73] Assignee: **Intel Corporation**, Santa Clara, Calif.

[21] Appl. No.: **730,065**

[22] Filed: **Oct. 15, 1996**

[51] **Int. Cl.**^{6} **H04N 7/167**

[52] **U.S. Cl.** **380/10; 380/20**

[58] **Field of Search** 380/20, 10

[56] **References Cited**

U.S. PATENT DOCUMENTS

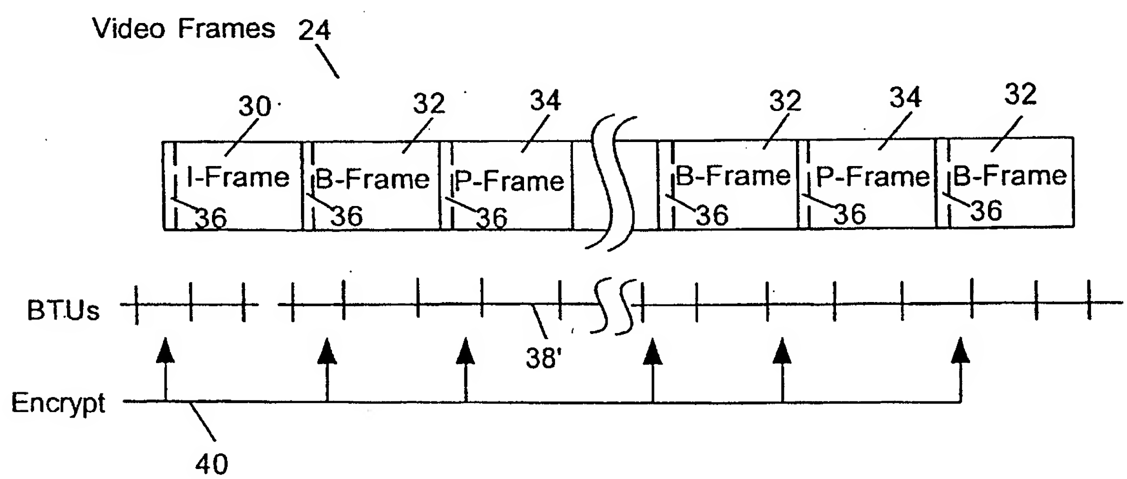
5,515,437	5/1996	Katta et al.	380/20
5,594,492	1/1997	O'Callaghan et al.	380/20
5,617,541	4/1997	Albanese et al.	380/42
5,621,794	4/1997	Matsuda et al.	380/20
5,621,799	4/1997	Katta et al.	380/20
5,625,693	4/1997	Rohatgi et al.	380/23
5,684,876	11/1997	Pinder et al.	380/37

Primary Examiner—Stephen C. Buczinski
Attorney, Agent, or Firm—Blakely, Sokoloff, Taylor & Zafman

[57] **ABSTRACT**

Basic transfer units (BTUs) of compressed video data of video images are selectively encrypted in accordance with an encryption policy to degrade the video images to at least a virtually useless state, if the selectively encrypted compressed video images were to be rendered without decryption. As a result, degradation that approximates the level provided by the total encryption approach is achieved, but requiring only a fraction of the processor cycle cost required by the total encryption approach, to decrypt and render the video images.

19 Claims, 6 Drawing Sheets



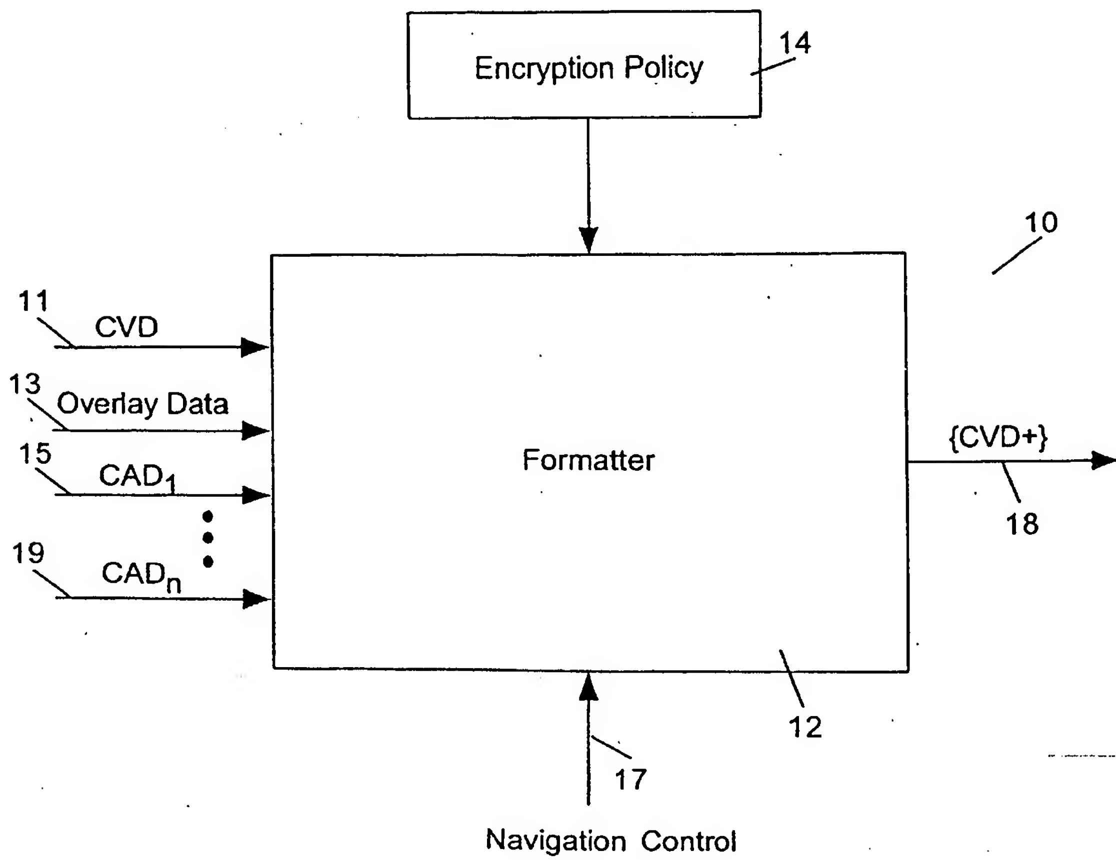

Encryption Policy
14
10
11
CVD
13
Overlay Data
15
CAD1
19
CADn
Formatter
{CVD+}
18
12
17
Navigation Control

Figure 1

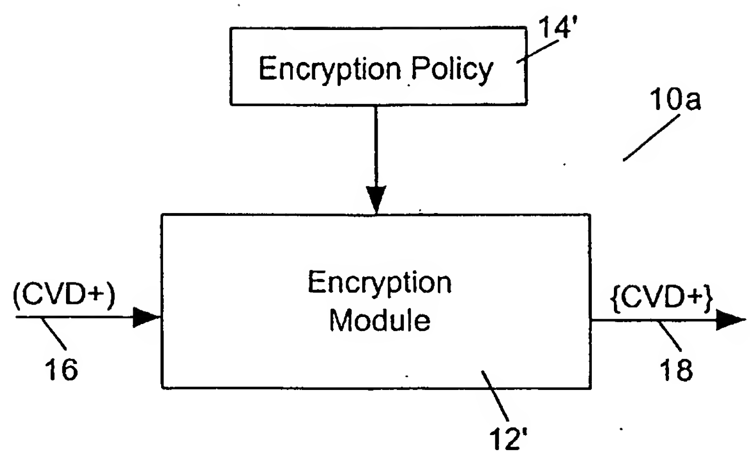


Figure 5

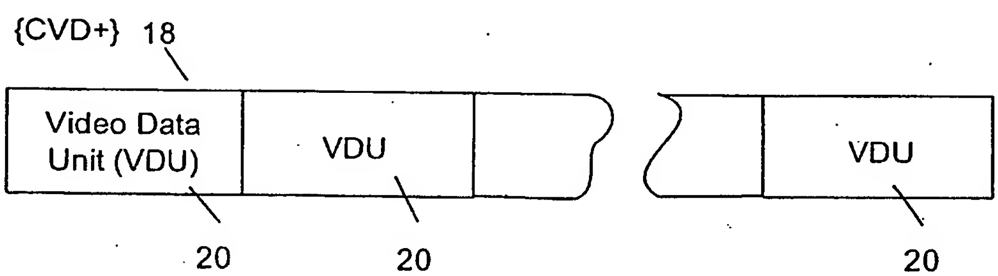


Figure 2

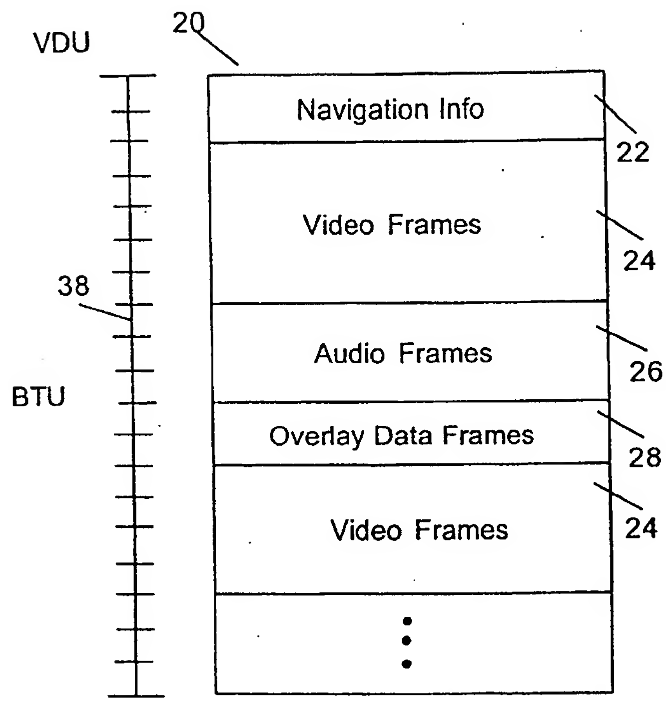


Figure 3

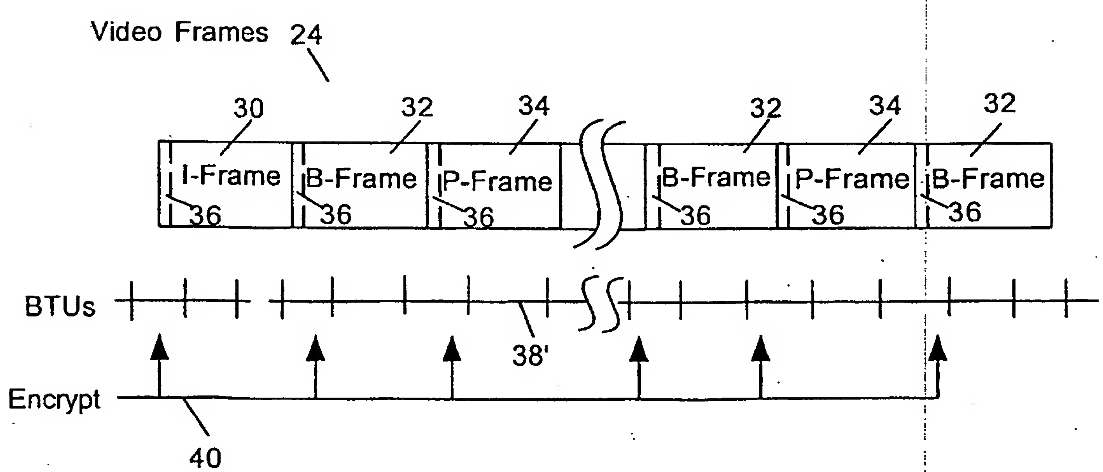


Figure 4

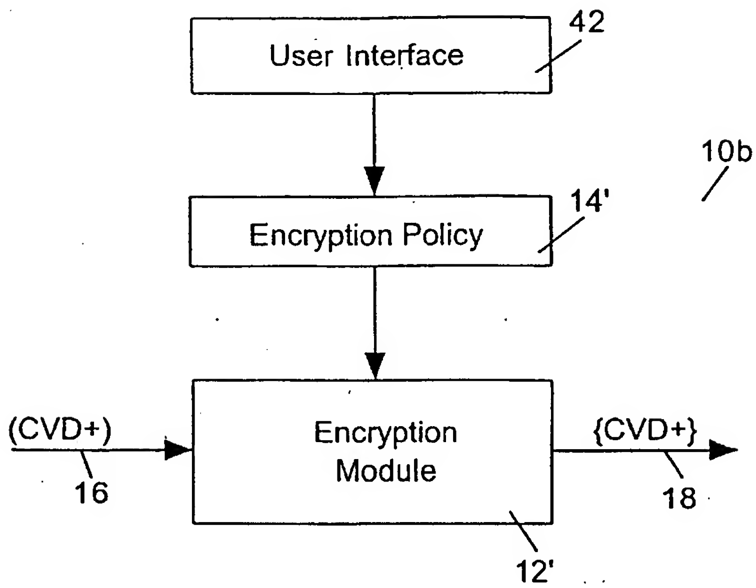


Figure 6

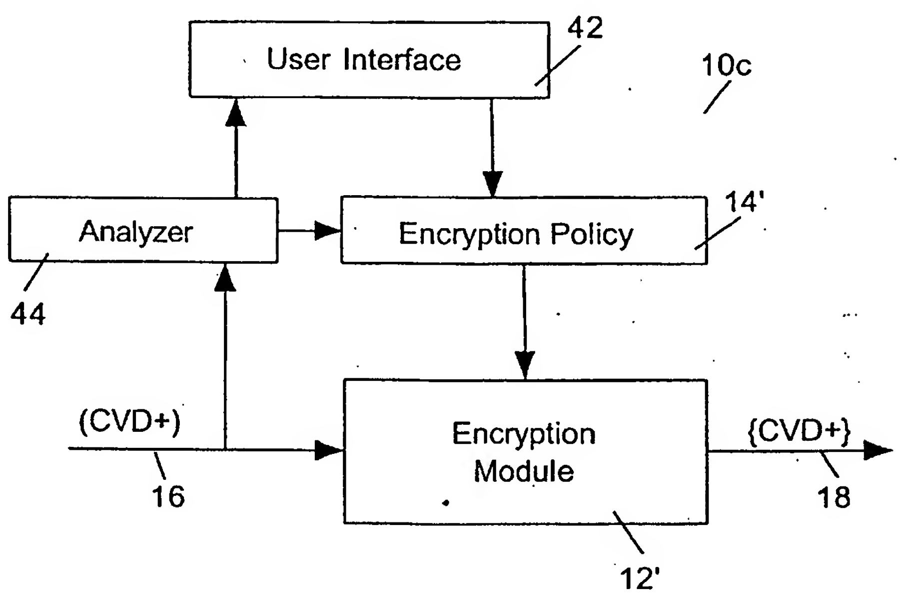


Figure 7

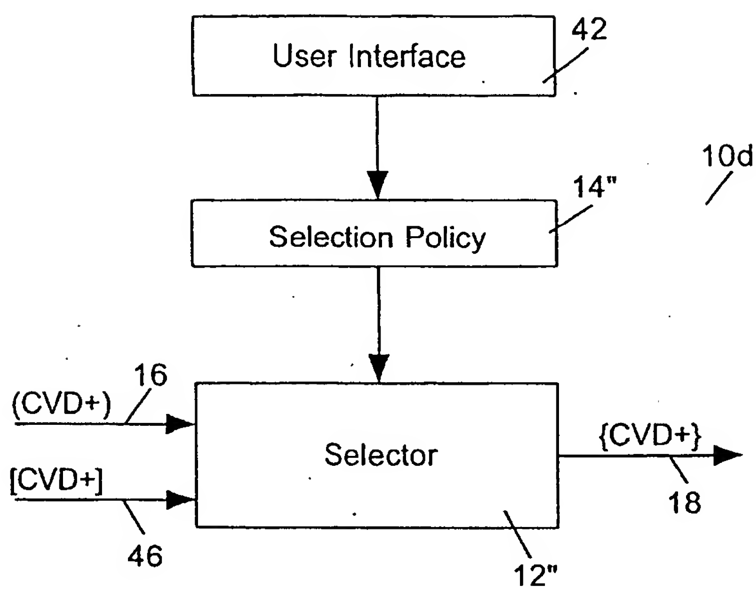


Figure 8

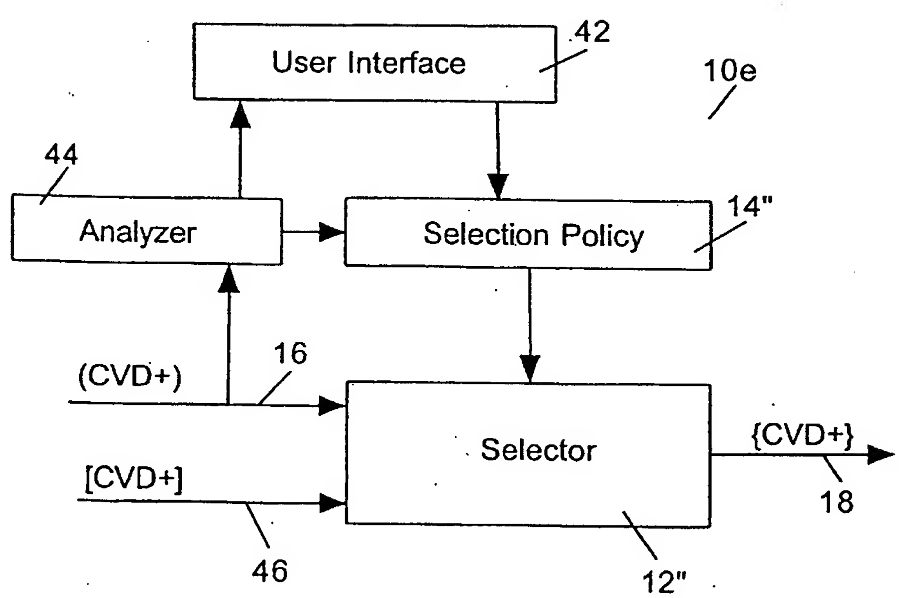


Figure 9

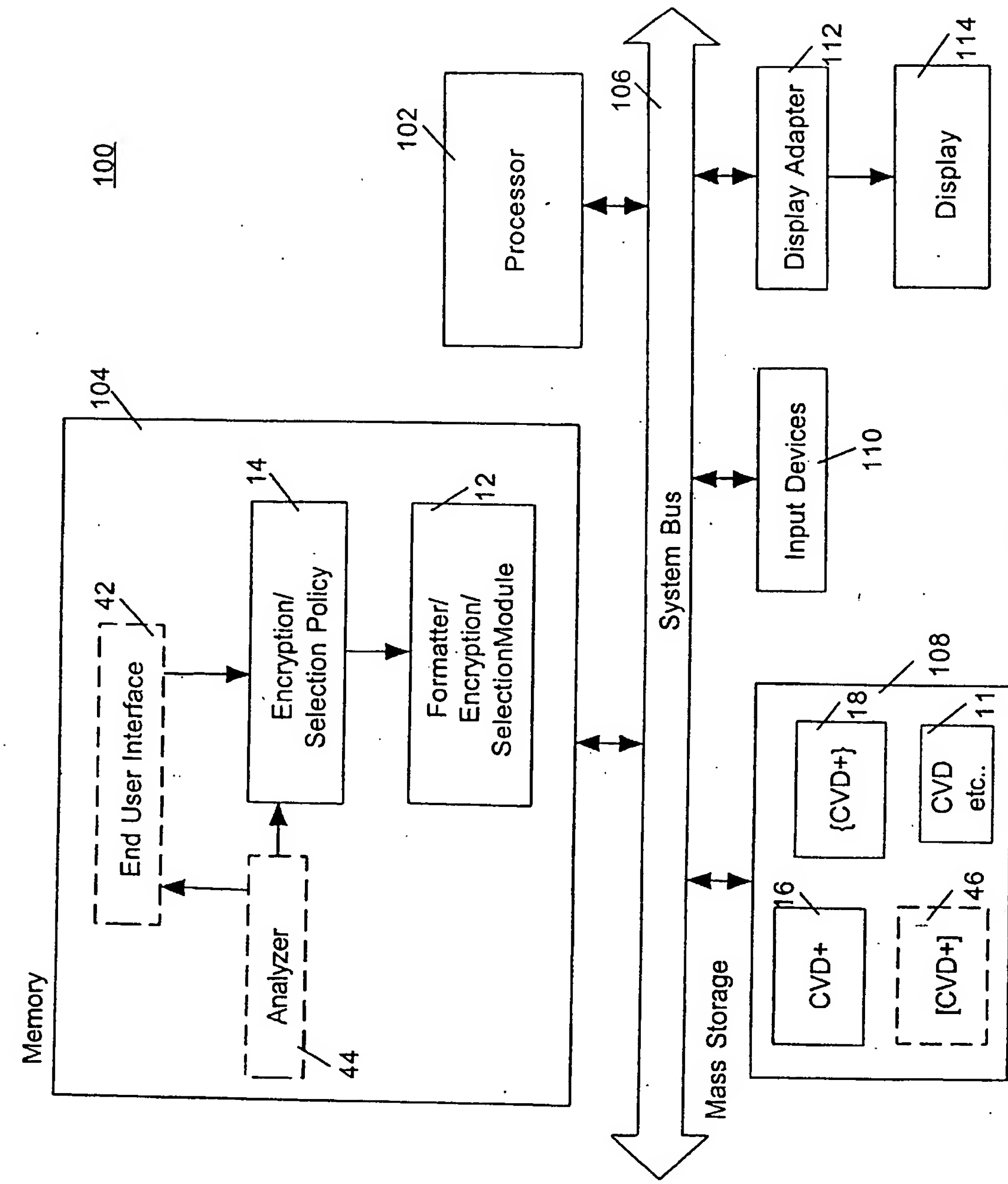

100
Memory
104
End User Interface
42
Encryption/
Selection Policy
14
Formatter/
Encryption/
SelectionModule
12
Analyzer
44
Processor
102
106
System Bus
Mass Storage
Display Adapter
112
Display
114
Input Devices
110
108
{CVD+}
18
CVD
etc..
11
CVD+
16
[CVD+]
46

Figure 10

POLICY BASED SELECTIVE ENCRYPTION OF COMPRESSED VIDEO DATA

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates to the art of data encryption, and in particular, to the art of encrypting video data for subsequent rendering on processor-based video systems.

2. Background of the Invention

There is substantial interest in the computer and entertainment industries in incorporating video data into multimedia and related applications for use on processor-based video systems. Potential growth in this area has been enabled by the development of video compression schemes that reduce the amount of video data required to display high quality video images, and by the development of storage media, such as digital video discs (DVDs), which can accommodate data (in compressed form) for an entire movie on a single compact disc.

With the compressed data of an entire movie readily available in a single compact disc, naturally content providers are extremely concerned with the unauthorized copying of the content. Thus, content providers are planning to encrypt the compressed data. As a result, the video data must be decrypted before they can be decompressed for rendering. The present practice is to encrypt the entire content. However, the present practice has the disadvantage of significantly burdening the processor during the decryption and decompression phase. Experience has shown that the decryption and decompression of a fully encrypted MPEG compressed movie can consume as much as over 30% of the available processor cycles, even with the latest high performance processors. Thus, a less burdening approach to preventing unauthorized copying of MPEG compressed video data is desirable.

SUMMARY OF THE INVENTION

Basic transfer units (BTUs) of compressed video data of video images are selectively encrypted in accordance with an encryption policy to degrade the video images to at least a virtually useless state, if the selectively encrypted compressed video images were to be rendered without decryption. As a result, degradation that approximates the level provided by the total encryption approach is achieved, but requiring only a fraction of the processor cycle cost required by the total encryption approach, to decrypt and render the video images.

In some embodiments, the encryption policy is predetermined, while in others, it is dynamically adjusted. In one embodiment, where the video images are MPEG compressed, all BTUs containing either the start code for a group of pictures or the start code for a particular frame are encrypted, to prevent recovery of the video frames. In an alternate embodiment, a fraction of the BTUs of an I-frame, and a fraction of the BTUs of a P-frame are encrypted, to destroy data references by future frames.

BRIEF DESCRIPTION OF DRAWINGS

The present invention will be described by way of exemplary embodiments, but not limitations, illustrated in the accompanying drawings in which like references denote similar elements, and in which:

FIG. 1 is a block diagram illustrating the present invention;

FIG. 2 illustrates a formatted stream of compressed video data in further details;

FIG. 3 illustrates one embodiment of a video data unit in further details;

FIG. 4 illustrates a group of pictures in a video object unit in further details;

FIGS. 5–9 are block diagrams illustrating various embodiments of the present invention; and

FIG. 10 illustrates one embodiment of a computer system suitable for practicing a software implementation of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

In the following description, various aspects of the present invention will be described. However, it will be apparent to those skilled in the art that the present invention may be practiced with only some or all aspects of the present invention. For purposes of explanation, specific numbers, materials and configurations are set forth in order to provide a thorough understanding of the present invention. However, it will also be apparent to one skilled in the art that the present invention may be practiced without the specific details. In other instances, well known features are omitted or simplified in order not to obscure the present invention.

Parts of the description will be presented in terms of operations performed by a computer system, using terms such as data, flags, bits, values, characters, strings, numbers and the like, consistent with the manner commonly employed by those skilled in the art to convey the substance of their work to others skilled in the art. As well understood by those skilled in the art, these quantities take the form of electrical, magnetic, or optical signals capable of being stored, transferred, combined, and otherwise manipulated through mechanical and electrical components of the computer system; and the term computer system include general purpose as well as special purpose data processing machines, systems, and the like, that are standalone, adjunct or embedded.

Referring now to FIG. **1**, wherein a block diagram illustrating the present invention is shown. As illustrated, formatter **12** of the present invention generates a formatted and partially encrypted stream of compressed video and related data {CVD+} **18** by selectively encrypting the basic transfer units (BTUs) of the compressed video and related data in accordance with an encryption policy **14**. The BTUs are formed using compressed video data (CVD) **11**, overlay data **13**, e.g. closed captions, compressed audio data (CAD1 . . . CADn) **15**, and navigation control **17**. As will be readily apparent from the description to follow, the video images of {CVD+} **18** are degraded to a level that approximates the degradation achieved by a total encryption approach, but requiring only a fraction of the processor cycle cost required by the total encryption approach to decrypt and render the video images.

In one embodiment, video images are compressed in accordance with one of the standards promulgated by the Moving Pictures Expert Group (MPEG, group ISO-IEC-JTC1 SC29/WG11) and the Joint Photographic Experts Group (JPEG, ISO/IEC International Standard 10918-1). The amount of spatial and temporal redundancy in the video data is reduced by application of lossy data transformations. Hereafter, MPEG is used to refer to MPEG-1 (ISO standard 11172), MPEG-2 (ISO standard 13818ISO), and JPEG compliant compression processes. Audio data are dolby AC3 or MPEG audio (MPEG1 or MPEG2). The selected BTUs are encrypted employing a stream cipher technique.

FIG. 2 illustrates the formatted and partially encrypted {CVD+} 18 in further details. As shown, {CVD+} 18 are formatted into video data units (VDUs) 20. In an embodiment where the compressed video data are organized in accordance with a DVD scheme, VDUs 20 are video object units (VOBUs). FIG. 3 illustrates one embodiment of a VDU 20, more specifically, a VOBU corresponding to a group of pictures, in further details. As shown, a VDU 20 or VOBU includes navigation information 22, multiple series of compressed video frames 24 interleaved with series of compressed audio frames 26 and series of compressed overlay data frames 28, spanning a number of BTUs 38. The constitution of a BTU 38 is application dependent. An example of a BTU 38 is a data packet. In a DVD application, each BTU 38 corresponds to a data packet for a disk sector, in the order of 2 k bytes. In a digital satellite service (DSS) application, each BTU 38 corresponds to a transmission packet.

FIG. 4 illustrates a series of compressed video frames 24 in a VOBU in further details. As shown, a series of compressed video frames 24 include a compressed I-frame 30, a number of compressed B-frames 32, and a number of compressed P-frames 34, spanning the BTUs 38'. Note that neither I-frame 30, B-frames 32, nor P-frames 34 are boundary aligned with BTUs 38'. Each of I-frame 30, B-frames 32, and P-frames 34 includes a start code 36. Each VOBU, that is, each group of pictures, also includes a start code (not shown).

Compressed I-frame 30 is generated in reference to itself, and is used as a reference frame for reconstituting the group of pictures during decompression. Compressed I-frame 30 includes almost exclusively "motionless" macroblocks. Compressed B-frames 32 are generated using motion compensated predictions referencing preceding as well as subsequent I-frames and P-frames. Compressed B-frames 32 include mostly backward as well as forward motion vectors. Compressed P-frames 34 are generated using motion compensated predictions referencing preceding I-frames and P-frames. Compressed P-frames 34 include mostly forward motion vectors, and a small amount of motionless macroblocks. The manner in which compressed I-frame 30, B-frames 32 and P-frames 34 may be generated is well known in the art.

FIG. 4 also illustrates one embodiment of an encryption policy 40. As shown, in accordance with the illustrated embodiment of encryption policy 40, each BTU 38' containing the start code of either a group of pictures, an I-frame 30, one of the B-frames 32 or one of the P-frames 34 is encrypted. As will be appreciated by those skilled in the art, by encrypting each of the BTUs 38' containing the start code of a group of pictures or the start code of a frame, frames 30, 32 and 34 are unrecoverable, that is effectively "destroyed", if the video images of partially encrypted {CVD+} 18 are rendered without decryption. As will be also appreciated by those skilled in the art, the number of BTUs 38' containing start codes for the various groups of pictures and the start codes of I, B and P-frame 30, 32 and 34 is a very small percentage of all BTUs 38'. In other words, only a few percent of the processor cycles required by the total encryption approach for decryption will be required to decrypt and render the partially encrypted {CVD+} 18, and yet the video images of partially encrypted {CVD+} 18 are degraded to the same level (that is, total "destruction") as the degradation achieved by the total encryption approach.

In an alternate embodiment, a fraction of the BTUs of either the I-frames 30 or the P-frames 34 are encrypted, to destroy data references for future frames. For example, every 3 of 4 BTUs 38' of an I-frame 30 within a VOBU, and every fourth BTU 38' of an P-frame 34 within the VOBU are encrypted, to destroy data references for future frames. None of the BTUs 38' of B-frames 32 within a VOBU are encrypted. Experience has shown that the number of BTUs 38' encrypted is a small percentage of all BTUs 38'. In other words, only a few percent of the processor cycles required by the total encryption approach for decryption will be required to decrypt and render the partially encrypted {CVD+} 18, and yet the video images of partially encrypted {CVD+} 18 are degraded to a level that is virtually useless, approximating the degradation achieved by the total encryption approach.

FIGS. 5–9 illustrates various embodiments of the present invention. FIG. 5 illustrates embodiment 10a wherein "formatter" 12 of FIG. 1 is replaced with encryption module 12'. Encryption module 12' performs the selective encryption based on encryption policy 14' as described earlier. However, encryption module 12' receives a formatted "clear" (that is, unencrypted) stream of compressed video and related data (CVD+) as input instead. FIG. 6 illustrates embodiment 10*b* wherein the present invention further includes user interface 42 for specifying encryption policy 14' for encryption modules 12'. FIG. 7 illustrates embodiment 10*c* wherein the present invention further includes analyzer 44 for analyzing the video images of CVD 16 to dynamically adjust encryption policy 14'. For examples, analyzer 44 may adjust encryption policy 14' based on certain frame statistics maintained for the video images of CVD 16. Alternatively, analyzer 44 may adjust encryption policy 14' based on the detection of a number constant or "slow" changing "landmarks", e.g. a mountain scene. Analyzer 44 may provide the analysis results to a user through user interface 42, who in turn will adjust encryption policy 14' through user interface 42. Alternatively, analyzer 44 may apply the analysis results directly to adjust encryption policy 14'. Statistical analysis of video images, as well as detection for "static" imagery in video images may be performed using any one of a number of these analysis techniques known in the art. Similarly, for both embodiments 10*a* and 10*b*, encryption module 12' may encrypt a selected BTU 38 using any number of encryption techniques known in the art.

FIG. 8 illustrates embodiment 10*d*, which is similar to embodiment 10*b*, except "encryption" module 12" is implemented with a selector, and "encryption policy" 14" is implemented with a selection policy. "Encryption" or selector module 12" is provided with fully encrypted video images of CVD+ 16, that is [CVD+] 46, as well as CVD+ 16. Whenever a BTU 38 is selected for encryption, instead of encrypting the selected BTU 38 on the fly, selector 12" simply selects and outputs the corresponding portion of [CVD+] 46. FIG. 9 illustrates embodiment 10*e*, which is similar to embodiment 10*c*, except "encryption" module 12" is implemented with a selector, and "encryption policy" 14" is implemented with a selection policy, as described earlier.

Encryption module 12' as well as "encryption" or selector module 12" may be implemented in hardware or software.

FIG. 10 illustrates one embodiment of a computer system suitable for practicing a software implementation of the present invention. As shown, for the illustrated embodiment, computer system 100 includes processor 102, memory 104, system bus 106, mass storage 108, input devices 110, display adapter 112 and display 114 coupled to each other as shown. Except for the manner they are used to practice the present invention, each of these elements 102–114 performs its corresponding conventional function known in the art, and each of these elements 102–114 is intended to represent a broad category of similar elements known in the art.

In particular, memory 104 is used to store a working copy each of formatter/encryption/selector module 12 and encryption/selection policy 14. Memory 104 may also be used to store a working copy each of end user interface 42 and analyzer 44. Mass storage 108 is used to store a working copy of CVD 11, CVD+16, {CVD+} 18, and/or [CVD+] 46. Alternatively, for systems with large memory or for small amount of video data, CVD 11, CVD+ 16, {CVD+} 18 and/or [CVD+] 46 may also be stored in memory 104. Finally, mass storage 108 may also be used to store a permanent copy of formatter/encryption/selector module 12 and encryption/selection policy 14, as well as end user interface 42 and analyzer 44.

While the present invention has been described in terms of the above illustrated embodiments, those skilled in the art will recognize that the invention is not limited to the embodiments described. The present invention may be practiced with modification and alteration within the spirit and scope of the appended claims. The description is thus to be regarded as illustrative instead of restrictive on the present invention.

Thus, a method and apparatus for policy based selective encryption of compressed video data has been described.

What is claimed is:

1. An apparatus comprising a formatter module for selectively encrypting basic transfer units (BTUs) of a stream of MPEG compressed video and related data in accordance with an encryption policy, the stream of MPEG compressed video and related data being organized into multiple video object units (VOBUs), with each VOBU being further organized into a plurality of BTUs, wherein the encryption policy prescribes for encryption of each BTU containing a start code of either a group of pictures, an I-frame, a B-frame or a P-frame.

2. An apparatus comprising a formatter module for selectively encrypting basic transfer units (BTUs) of a stream of MPEG compressed video and related data in accordance with an encryption policy, the stream of MPEG compressed video and related data being organized into multiple video object units (VOBUs), with each VOBU being further organized into a plurality of BTUs, wherein the encryption policy prescribes for encryption of a fraction of the BTUs of an I-frame within a VOBU.

3. The apparatus as set forth in claim 2, wherein

the encryption policy prescribes for encryption of three of every four BTUs of an I-frame within a VOBU.

4. An apparatus comprising a formatter module for selectively encrypting basic transfer units (BTUs) of a stream of MPEG compressed video and related data in accordance with an encryption policy, the stream of MPEG compressed video and related data being organized into multiple video object units (VOBUs), with each VOBU being further organized into a plurality of BTUs, wherein the encryption policy prescribes for encryption of a fraction of the BTUs of a P-frame within a VOBU.

5. The apparatus as set forth in claim 4, wherein

the encryption policy prescribes for encryption of every fourth BTU of a P-frame within a VOBU.

6. An apparatus comprising an encryption module for selectively encrypting basic transfer units (BTUs) of a stream of MPEG compressed video data in accordance with an encryption policy, the stream of MPEG compressed video data being organized into multiple video object units (VOBUs), with each VOBU being further organized into a plurality of BTUs, wherein the encryption policy prescribes for encryption of each BTU containing a start code of either a group of pictures, an I-frame, a B-frame or a P-frame within a VOBU.

7. An apparatus comprising an encryption module for selectively encrypting basic transfer units (BTUs) of a stream of MPEG compressed video data in accordance with an encryption policy, the stream of MPEG compressed video data being organized into multiple video object units (VOBUs), with each VOBU being further organized into a plurality of BTUs, wherein the encryption policy prescribes for encryption of a fraction of the BTUs of an I-frame within a VOBU.

8. The apparatus as set forth in claim 7, wherein

the encryption policy prescribes for encryption of three of every four BTUs of an I-frame, within a VOBU.

9. An apparatus comprising an encryption module for selectively encrypting basic transfer units (BTUs) of a stream of MPEG compressed video data in accordance with an encryption policy, the stream of MPEG compressed video data being organized into multiple video object units (VOBUs), with each VOBU being further organized into a plurality of BTUs, wherein the encryption policy prescribes for encryption of a fraction of the BTUs of a P-frame within a VOBU.

10. The apparatus as set forth in claim 9, wherein

the encryption policy prescribes for encryption of every fourth BTU of a P-frame within a VOBU.

11. An apparatus comprising a selector module for generating a partially encrypted stream of MPEG compressed video data by selectively outputting basic transfer units (BTUs) of a formatted (but unencrypted) stream of MPEG compressed video data and BTUs of a formatted and encrypted stream of MPEG compressed video data, in accordance with a selection policy, each of the formatted unencrypted and encrypted streams of MPEG compressed video data being organized in multiple video object units (VOBUs), with each VOBU being further organized into a plurality of BTUs, wherein the selection policy prescribes for selection of each BTU containing a start code of either a group of pictures, an I-frame, a B-frame or a P-frame within a VOBU from the formatted encrypted stream of MPEG compressed video data.

12. An apparatus comprising a selector module for generating a partially encrypted stream of MPEG compressed video data by selectively outputting basic transfer units (BTUs) of a formatted (but unencrypted) stream of MPEG compressed video data and BTUs of a formatted and encrypted stream of MPEG compressed video data, in accordance with a selection policy, each of the formatted unencrypted and encrypted streams of MPEG compressed video data being organized in multiple video object units (VOBUs), with each VOBU being further organized into a plurality of BTUs, wherein the selection policy prescribes for selection of a fraction of the BTUs of an I-frame within a VOBU from the formatted encrypted stream of MPEG compressed video data.

13. The apparatus as set forth in claim 12, wherein p1 the selection policy prescribes for selection of three of every four BTUs of an I-frame, within a VOBU, from the formatted encrypted stream of MPEG compressed video data.

14. An apparatus comprising a selector module for generating a partially encrypted stream of MPEG compressed video data by selectively outputting basic transfer units (BTUs) of a formatted (but unencrypted) stream of MPEG compressed video data and BTUs of a formatted and encrypted stream of MPEG compressed video data, in accordance with a selection policy, each of the formatted unencrypted and encrypted streams of MPEG compressed video data being organized in multiple video object units (VOBUs), with each VOBU being further organized into a

plurality of BTUs, wherein the selection policy prescribes for selection of a fraction of the BTUs of a P-frame within a VOBU from the formatted encrypted streams of the MPEG compressed video data.

15. The apparatus as set forth in claim 14, wherein

the selection policy prescribes for encryption of every fourth BTU of a P-frame within a VOBU from the formatted encrypted stream of MPEG compressed video data.

16. An apparatus comprising

a storage medium having stored therein a plurality of programming instructions for implementing an encryption function for selectively encrypting basic transfer units (BTUs) of MPEG compressed video data, in accordance with an encryption policy, the MPEG compressed video data being organized into multiple video object units (VOBUs), with each VOBU being further organized into a plurality of BTUs, wherein the encryption policy prescribes for encryption of each BTU containing a start code of a group of pictures or a start code of a frame within a VOBU; and

an execution unit coupled to the storage medium for executing the plurality of programming instructions during operation.

17. The apparatus as set forth in claim 16, wherein

the encryption policy prescribes for encryption of a fraction of the BTUs of an I-frame or a P-frame within a VOBU.

18. An apparatus comprising

a storage medium having stored therein a plurality of programming instructions for implementing a selection function for generating a partially encrypted stream of MPEG compressed video data by selectively outputting basic transfer units (BTUs) of an unencrypted stream of MPEG compressed video data and BTUs of an encrypted stream of MPEG compressed video data, in accordance with a selection policy, each of the unencrypted and encrypted streams of MPEG compressed video data being organized into multiple video object units (VOBUs), with each VOBU further being organized into a plurality of BTUs, wherein, the selection policy prescribes for selection of each BTU containing a start code a group of pictures or a start code of a frame within a VOBU, from the encrypted stream of compressed video data;

an execution unit coupled to the storage medium for executing the plurality of programming instructions during operation.

19. The apparatus as set forth in claim 18, wherein

the selection policy prescribes for selection of a fraction of the BTUs of either an I-frame or a P-frame within a VOBU, from the encrypted streams of the MPEG compressed video data.

* * * * *